Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims

1. (Cancelled)

2. (Currently Amended) The method according to claim ~~1~~ 10 wherein said open key is transmitted ~~to the recipient~~ by adding it to ~~the~~ a ~~stream~~ header ~~and then extracted from the stream header at the recipient's station for decryption~~ of the transmission.

3. (Currently Amended) The method according to claim ~~1~~ 9 wherein said base key is encrypted using a public key encryption algorithm ~~in conjunction with the recipient's public key and wherein said open key is decrypted using said public key encryption algorithm in conjunction with the recipient's private key~~.

4. (Currently Amended) The method according to claim ~~1~~ 9 wherein said packet data is encrypted using a symmetric encryption algorithm in conjunction with said packet key ~~and said encrypted data is decrypted at the recipient's station using said symmetric encryption algorithm in conjunction with said recreated packet key~~.

5. (Currently Amended) The method according to claim ~~1~~ 11 wherein the secure hash is based on a hash function selected from the group comprising ~~used to create and re-establish said packet key is~~ SHA-1 ~~or~~ and MD5.

6. (Cancelled)

7. (Cancelled)

8. (Cancelled)

9. (New) A method for securely transmitting streaming media, the method comprising:

generating a random base key;

encrypting the streaming media by creating a packet key for each data packet of the streaming media and encrypting each data packet using the packet key, the packet key being based on the base key and unique packet tags assigned to each data packet; and

transmitting the encrypted data packets, the packet key, the base key, and the unique packet tags to a recipient.

10. (New) The method of claim 9 further comprising encrypting the random base key prior to transmission, thus creating an open key.

11. (New) The method of claim 9 wherein the packet key is based on a secure hash of the base key and unique packet tags assigned to each data packet.

12. (New) The method according to claim 3 wherein said public key encryption algorithm is asymmetric.

13. (New) A method of receiving encrypted streaming media, the method comprising:

receiving an encrypted packet stream and an encrypted base key, the packet stream comprising a plurality of packets, each packet comprising encrypted packet information and a unique tag value;

extracting the unique tag value from each packet;

computing a packet key for each packet based on the unique tag value and the encrypted

base key; and

decrypting the packet information using the corresponding packet key.

14. (New) The method according to claim 13 wherein said base key is encrypted using a public key encryption algorithm.

15. (New) The method of claim 13 wherein the computation of the packet key is based on a secure hash of the base key and the unique packet tags assigned to each data packet.

16. (New) The method according to claim 15 wherein the secure hash is based on a hash function selected from the group comprising SHA-1 and MD5.